

AUSA: April N. Russo

Telephone: (313) 226-9100

AO 106 (Rev. 04/10) Application for a Search Warrant

Special Agent:

Adam Christensen (FBI)

Telephone: (313) 965-2323

**UNITED STATES DISTRICT COURT**  
for the  
Eastern District of Michigan

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )

one Samsung SM-J320V cellular phone, one Acer Aspire )  
ZRQ laptop, and one Ativa SD card (more fully described )  
in Attachment A) )

Case: 2:19-mc-51458 - 1  
Case No. Assigned To : Edmunds, Nancy G.  
Assign. Date : 10/3/2019  
IN RE: SEALED MATTER (CMC)

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

*Offense Description*

18 USC §§ 2251(a); 2422

Production of child pornography; Coercion and enticement

18 USC §2252A

Receipt, possession, and distribution of child pornography

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.  
☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



*Applicant's signature*

Adam Christensen, Special Agent (FBI)

*Printed name and title*

Sworn to before me and signed in my presence  
and/or by reliable electronic means.

Date: October 3, 2019

City and state: Detroit, Michigan



*Judge's signature*

Hon. R. Steven Whalen, U. S. Magistrate Judge

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**  
**INTRODUCTION**

I, Adam Christensen, having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a Special Agent of the FBI since 2010, and am currently assigned to the Detroit Division, Southeast Michigan Trafficking and Exploitation Crimes Taskforce. While employed by the FBI, I have investigated federal criminal violations related to child exploitation, and child pornography. I have gained experience through training and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2251(a) and (e) (producing, attempting to produce, and conspiracy to produce child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive

and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography); 18 U.S.C. § 2422 (coercion and enticement); and § 2252A(g)(2) (participating in a child pornography enterprise) are located within **the electronic media seized from Richard Eby at the Fort Lauderdale-Hollywood International Airport on June 25, 2019 by Homeland Security Investigations** (hereinafter referred to as the SUBJECT DEVICES). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT DEVICES, as further described in Attachment A, incorporated herein by reference, which are currently located in the Eastern District of Michigan.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for the limited purpose of

securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

### **RELEVANT STATUTES**

4. This investigation concerns alleged violations of : 18 U.S.C. § 2251(a) and (e) (producing, attempting to produce, and conspiracy to produce child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography); 18 U.S.C. § 2422 (coercion and enticement); and 18 U.S.C. § 2252A(g)(2) (participating in a child pornography enterprise) (hereafter the Specified Federal Offenses).

### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

5. Through my experience and training, and that of other FBI Special Agents, the following traits and characteristics are generally found to exist and be true in cases involving individuals who collect child pornography:

- The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification

and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

- Most of the individuals who collect child pornography often seek out likeminded individuals, either in person or on the internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different internet based vehicles used by such individuals to communicate with each other include, but are not limited to, websites, email, email groups, bulletin boards, internet chat programs, newsgroups, instant messaging, and other similar vehicles.
- Many of the individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

- Many of the individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections from discovery, theft, and damage. Your Affiant knows from training and experience that such individuals have been known to maintain possession of their child pornography for years, or even decades. They almost always maintain their collections in the privacy and security of their homes or other secure locations, such as their work spaces or on their person.
- Moreover, your affiant knows that persons who collect child pornography often transfer their material to hard drives, USBs, or other electronic devices in order to create storage space for additional child pornography and in order to backup the child pornography they have collected.

6. Your Affiant believes the subject of the instant investigation to be a collector of child pornography because, as further described herein, the subject has communicated with other like-minded individuals to carry out a scheme to create, share, and view child pornography. Specifically, the members of this group primarily operate by convincing minor females to visit chatrooms on Website A, enticing them to engage in masturbation and other sexual acts while they are on webcam, and then recording

the activity. I know the majority of individuals who routinely visit websites like Website A, which are primarily devoted to child pornography and the online enticement of minors, are collectors of child pornography. Moreover, I know, based on the investigation of many other offenders on Website A, that numerous Website A offenders stored child pornography on multiple electronic devices and transferred child pornography from one device to another.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

7. As described above and in Attachment B, this application seeks permission to search for evidence of violations of the Specified Federal Offenses that might be found on the SUBJECT DEVICES, in whatever form they are found. One form in which the records will be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media and the copying of electronically stored information, all under Rule 41(e)(2)(B).

8. *Probable cause.* I submit that there is probable cause to believe evidence of violations of the Specified Federal Offenses will be stored on the SUBJECT DEVICES, for at least the following reasons:

- Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after

they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this



evidence, because special software is typically required for that task.

However, it is technically possible to delete this information.

- Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

9. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any of the SUBJECT DEVICES because:

- Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the

attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element, or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate

how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer

may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

10. I know that when an individual uses a computer to create, access, receive, and/or distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense (for example, the computer is used to access the internet to record, download, access with the intent to view, or distribute child pornography). The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: child pornography images and videos, data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the

offense.

*11. Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of electronic evidence for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time at the site of the search is not feasible. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that

information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

**12. Nature of examination.** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or

information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

### **INTRODUCTION TO THE SOCIAL MEDIA PLATFORMS IN THIS CASE AND THE INVESTIGATION**

13. This investigation focuses on a group of Website A<sup>1</sup> users that have conspired together to target and recruit minor females to join Website A chatrooms in order to persuade and entice these girls to engage in sexually explicit conduct on webcam so that the group members can view and record it. This group uses at least the following internet platforms: Website A and MyLOL.

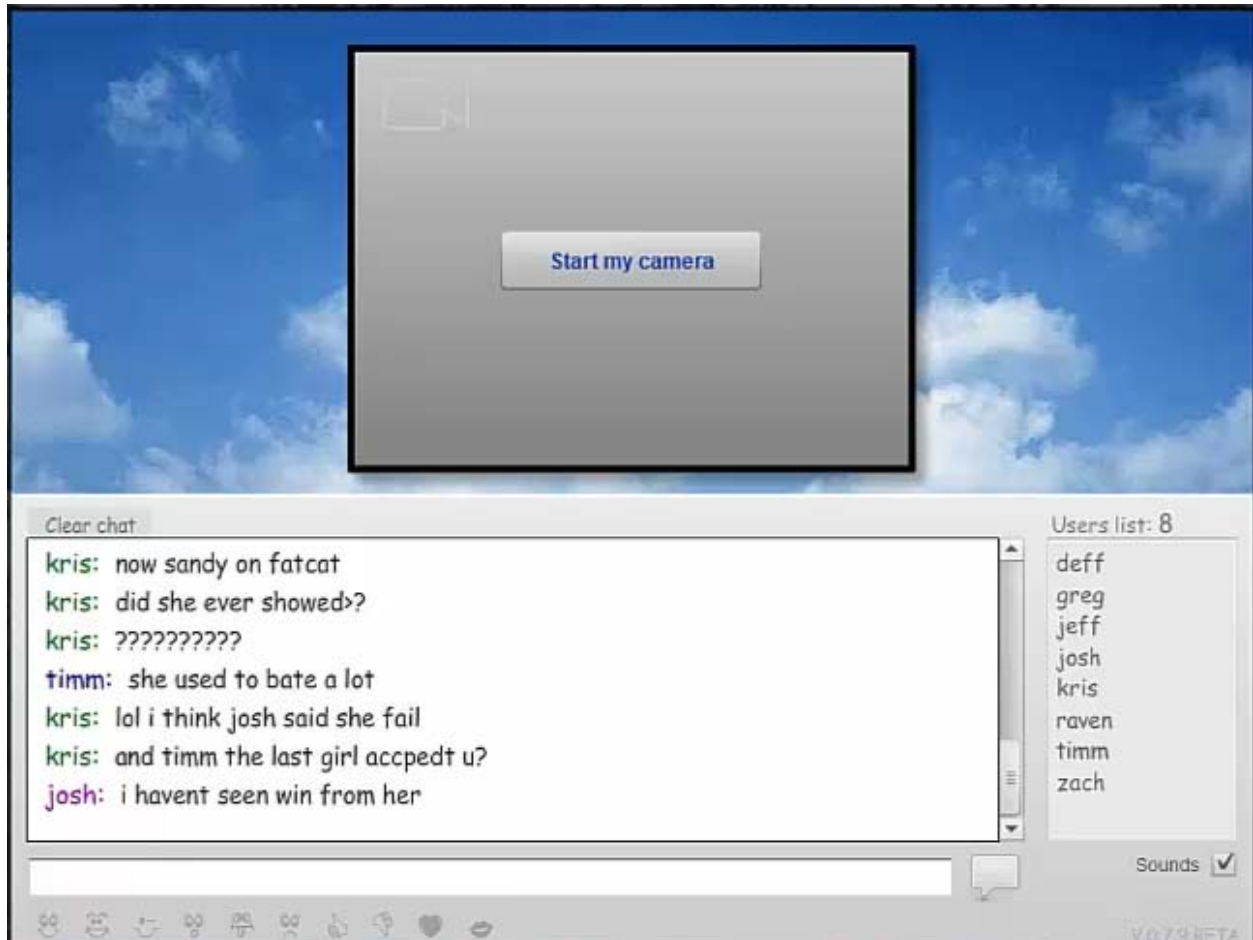
14. Website A is a chatroom-based social media platform where people, using usernames of their choosing, enter chatrooms and communicate with other users in real time. The chatrooms have a list of users in the lower right corner of the screen, an active chat conversation on the lower left corner of the screen, and a large space above these for individuals to live stream their activities via web camera. The image below is an example of a chatroom with no users on webcam. In each chatroom, at any

---

<sup>1</sup> The true name of Website A is known to law enforcement but is not being disclosed in this affidavit because this investigation is ongoing and disclosure of its name may



given time, up to two users could broadcast their activities via web camera. When two users were broadcasting in a room like the one below at the same time, the screen would split into two boxes, and their videos would play side by side on the top of the screen.



15. The hosting service for Website A is located in Spain. The Spanish National Police, based on requests by the FBI, obtained logs from the hosting service of Website A. These logs covered the periods of April 1, 2015, up to September 30,

---

impede future investigatory efforts.

2017 and January 1, 2018 to February 19, 2019. The logs listed the IP address utilized by a user to perform an activity on the website. When a user logged into a room, the specific name of the room and the date and time that the IP was utilized to log into that room was specified. When a user streamed on camera in a chatroom, the logs provided that user's chosen username, the type of webcam used, the user's IP address, the date and time the user was actively streaming on camera, and the total number of users in the chatroom at that time. For users that did not stream on camera in the chatroom, only the user's IP address—and not their username—appeared in the logs.

16. MyLOL.com is a website designed to facilitate teen dating and describes itself as “the #1 teen dating site in the US, Australia, UK, and Canada.” Users on MyLOL.com create a profile with their age and where they are from. The users can then message or chat with each other. It is designed much like other online dating websites, but with the caveat that members be between the age of 13 and 19 years old at the time that they sign up for the service.

17. As explained in more detail below, the FBI investigation has revealed that groups of users on Website A coordinate together to recruit, entice, and coerce minor females into producing child pornography through the webcam contained in the targeted minor females' computers. These groups of users on Website A have specific

roles to play in the mission of convincing the targeted minor females to engage in sexually explicit conduct so that the group members can record it.

### **PROBABLE CAUSE**

#### ***FBI's Identification of the "Fans" Group on Website A***

18. On November 16, 2015, the FBI executed a search warrant in the Eastern District of Michigan on the residence of the subject of a separate, nationwide child pornography investigation. The subject (hereafter "S1")<sup>2</sup> informed agents that he was a member of a group of individuals that uses the internet to entice minors to engage in sexually explicit conduct via web camera. The members of this group primarily operate by convincing minor females to visit chatrooms on Website A. Once the girls arrive in the chatroom,<sup>3</sup> group members worked together to convince them to undress and masturbate on camera. Everyone present in the chatroom has the ability to watch the girls engaged in these acts, and the group members record the girls. Some of the group members distribute the recordings to other people. S1 identified that many of the chatrooms used by the group had the word "fans" in the title of the chatroom. S1 stated that he knew that other groups like his existed and operated in a similar fashion

---

<sup>2</sup> S1 and S2's identities are known to law enforcement but not revealed to protect the integrity of the ongoing investigation.

<sup>3</sup> The web address for the chatrooms on Website A is always the name of the website/the name of the room.

on Website A.

19. According to S1, the various roles in his group included: “hunters,” “talkers,” “loopers,” and “watchers.”

- a. The “hunters” visit social media websites commonly used by their minor victims (including MyLOL.com) to interact with the minors. They are in charge of convincing minors to log-on to Website A. They provide the minor females with a link to a specific chatroom that they or another group member create on Website A.
- b. Once the targeted minors log-on to Website A, the “talkers” take over the primary job of conversing with them. “Talkers” ask the targeted minors to do “dares” which escalate into sexual activity. “Talkers” attempt to convince the targeted minors to engage in sexually explicit conduct via webcam.
- c. If the “talkers” fail to convince the targeted minor to engage in sexual activity on camera, the “loopers” get involved. The “looper” plays a previously recorded video of a different minor chatting and/or performing sexual acts in a chatroom. The “looper” pretends to be the minor depicted in the video that is broadcast to the targeted minor victim as if it is occurring in real-time. The “looper” plays the video or “loop”

to entice the targeted minor in the chatroom to engage in sexual activity on camera, just as the minor in the previously recorded video had done. The “loopers” use software programs, the most common being ManyCam Virtual Webcam, and others include Splitcamera, MiniCam and WebcamMax, to make it appear as if the previously recorded videos they are playing are being broadcast in real-time in the chatroom. In other words, when the targeted minor is in the chatroom on Website A, she believes the video being displayed by the “looper” is in fact another minor actively engaged in the chatroom on camera in real time.

- d. Finally, “watchers” are in charge of security for the group. They watch the users coming and going from the chatroom to make sure that no suspected law enforcement members or other unwanted persons access the room.
- e. The investigation thus far has revealed that all of the core members of this group, regardless of their role, recorded the sexual activity engaged in by the targeted minors on camera. Recording this sexual activity is known as “capturing” or “capping” the webcam activity.

20. S1 gave the FBI permission to assume his online identity on Website A. For a period of approximately three weeks in December of 2015, an FBI agent (hereafter the

UCA) went undercover, logging into numerous chatrooms on Website A utilizing the username and passwords<sup>4</sup> of S1.

21. This undercover investigation confirmed S1's allegations about the group, and provided additional evidence of the online exploitation of preteen and teenage minor girls by members of the group identified by S1 (hereafter the "Fans Group"). During the undercover investigation, the UCA observed users on Website A successfully entice at least ten minor females to produce child pornography. From the information provided by S1, the undercover operation, and traditional FBI investigative techniques, the FBI identified and arrested several members of the Fans Group. Six American-based members of the Fans Group (including S1) were convicted in the Eastern District of Michigan of child exploitation enterprise based on their conduct on Website A. Beyond the six American-based members of the group, foreign-based members have been identified as well. The FBI has sent information about these foreign-based offenders to law enforcement in those countries. Over 30 minor victims of the Fans Group that are currently residing in the United States have been identified. Numerous others reside in foreign countries or remain unidentified.

---

<sup>4</sup> Only a few of the rooms on Website A required a password. A user can type in the username of their choosing in the particular chatrooms on Website A and can switch usernames as frequently as they desire. Usernames are not exclusive on Website A. However, the UCA observed that most users consistently used the same usernames for their activities on Website A.

22. During the undercover sessions, the UCA observed numerous individuals and groups, outside of the Fans Group, that used similar terminology and methodology and were involved in the enticement of minors to produce child pornography. For example, the UCA observed that users on Website A commonly used the word “win” to describe getting a girl to engage in sexual activity, “cap” or “capture” to describe a recording, and the abbreviation “bate” for the word masturbate. The UCA observed enticement of minors and attempted production and/or production of child pornography in dozens of chatrooms by persons using numerous different user names. From his observations, the UCA concluded that Website A was primarily devoted to the online enticement of minor females and the production of child pornography. The UCA also concluded that several other groups of individuals were colluding together to exploit girls on Website A in a similar manner as the Fans Group. This conclusion was consistent with information provided by S1 and other individuals who have been interviewed regarding their activity on Website A, and with other information obtained by law enforcement during the ongoing investigation of Website A.

23. The FBI learned that one of these other similar groups typically coordinated their sexually exploitative activity on Website A through a group chat on the internet platform Skype (hereafter the Skype Group). The FBI recovered and reviewed the

content of several years of the Skype Group's chat conversations. From those conversations, it was evident that, like the Fans Group, the Skype Group targeted minor females on Website A in order to get them to engage in masturbation and other sexual activity on webcam so that group members could record it. The investigation into the Skype Group resulted in the identification and arrest of eight of its members.<sup>5</sup> All eight have been convicted in the Eastern District of Michigan for child exploitation enterprise. A partial forensic examination of the devices that were seized during search warrants executed at the residences of the Skype Group members has thus far revealed that all eight appear to have recorded minors engaged in masturbation while those minors were on webcam, and many of the recordings appear to be from Website A. Interviews with several group members confirmed the FBI's conclusions about the group and its purpose.

#### ***FBI's Identification of the Chats Group***

24. A review of the lengthy Skype-based conversations among the Skype group members revealed discussions regarding other groups of like-minded individuals operating on Website A. One such group was referred to by the Skype group as

---

<sup>5</sup> Like the Fans Group, the Skype Group has several members who are believed to be residing in other countries. The investigation into the whereabouts of those individuals and additional possible United States' members is ongoing.



“zhit’s group.” One of the first references to Zhit’s Group was in a conversation that was dated February 10, 2016:

llama.4u:	I’m talking to <b>WHISPER20</b> <sup>6</sup>
mudd.pie:	lol [MV] <sup>7</sup> in bithc [sic] mode
benji00006:	[MV] giving a speech
llama.4u:	WHAT A FAGGOT
benji00006:	speech*
aiden.flyer:	I left that room after I saw shew was on
aiden.flyer:	whos wisper?
llama.4u:	some fag he’s fucking lame
crash_n_burn101:	lol
llama.4u:	he’s on another group
benji00006:	he is on g0ds rooms
benji00006:	also
llama.4u:	G0d’s and <b>ZHIT/LAK/PERP6969/POORBOY</b>
	group
aiden.flyer:	oh
crash_n_burn101:	i can’t locate kittybabe
benji00006:	the lamest guys are on the most groups
benji00006:	like <b>VIN</b>
mudd.pie:	did we send her to them..... kinda like a ‘smart weapon’
llama.4u:	<b>VIN</b> is there to
llama.4u:	in that group
llama.4u:	;D
aiden.flyer:	where isn’t <b>VIN</b> :P
llama.4u:	but he’s only there when there’s a bate then leave
aiden.flyer:	and he doesn’t talk
benji00006:	well theres lots of win there, we suck :P

---

<sup>6</sup> Group members’ names were not necessarily capitalized or in bold in the original affidavit but are capitalized and in bold here for ease of reading and identification.

<sup>7</sup> The names of individuals believed to minors are redacted and replaced with MV to protect their privacy. The true age and location of these individuals is unknown, and the belief that they are minors is based on the general purpose and objective of the group.

aiden.flyer: oh really?  
 llama.4u: one girl just bated for them  
 mudd.pie: hope back  
 benji00006: is pass off chill\_party?  
 llama.4u: [provided an image]  
 crash\_n\_burn101: who is that??  
 llama.4u: a girl that just bate for **ZHIT**'s group  
 llama.4u: she's a tattoo :P  
 benji00006: but still nice  
 asddffhgrhfs.trtghgj: what does it say on her tummy? "I love you Daddy Clay"? :O :O  
 aiden.flyer: cum here  
 crash\_n\_burn101: (rofl)  
 crash\_n\_burn101: they got her from cb?  
 crash\_n\_burn101: (cwl)  
 llama.4u: mylol

25. The FBI observed another Skype group conversation, dated February 18, 2016, regarding Zhit's Group a few days later:

llama.4u: I was talking to **ZHIT** yesterday, and he tho we hoarder his girls... I told him to look in his own chat for hoarders... The cunt was like... well there's some guys I don't fucking know who they are  
 llama.4u: hoarded\*  
 llama.4u: and **LAK** was like I WANNA SEE [MV] SHOW ME NOW  
 erenxjaeger: xD  
 tomarsplz: xD  
 crash\_n\_burn101: lol  
 mudd.pied: HA  
 llama.4u: **ZHIT** seem ok with every group in their own rooms, **LAK** was like idc I'm in 5 groups and I'll be in your group too... "No you don't"... omg you are so sassy about the girls

crash\_n\_burn101: sounds like **LAK** is one of those bm'er  
aiden.flyer: well, **LAK** is under...  
llama.4u: no he's plain retarded

26. A third example was from March 7, 2016:

mudd.pie: okay, maybe not old enough to read  
aiden.flyer: old enough for **ZHIT**s group  
mudd.pie: sadly true  
llama.4u: **ZHIT** does 16+  
llama.4u: **LAK** doesn't give a fuck  
aiden.flyer: **LAK ZHIT**s, aren't they all the same group?  
llama.4u: yep  
llama.4u: but **ZHIT** only links girls 15/16+  
mudd.pie: **ZHIT**'s group on the other hand

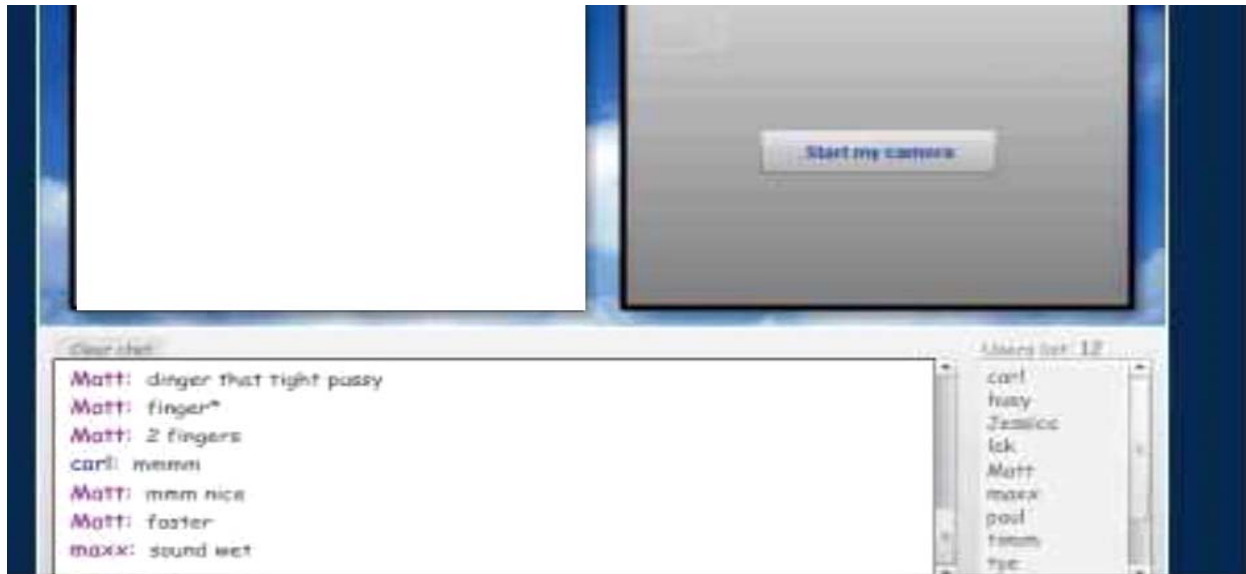
27. Several other conversations from the Skype group referred to **ZHIT**'s group, including identifying some of its members. From the FBI's review of all of the Skype group's conversations, the FBI concluded that Zhit's group consisted of at least **ZHIT, LAK, WHISPER20, PERP6969, POORBOY, TURTLE, ROB, CONNOR, DAVE, VIN, JOHN, and STIG**. Moreover, from these conversations, the FBI determined that Zhit's Group, like the Fans group and the Skype group, sought to recruit, entice, and coerce girls to engage in sexually explicit activity on camera on Website A.

28. Forensic evidence from the computers of the Skype group likewise showed evidence of Zhit's group engaging in the sexual exploitation of children. Usernames

of several of Zhit's group were in rooms with minors who were enticed to engage in sexual activity. First, a video entitled [MV].avi depicts a female believed to be between 14 and 17 years old on webcam in a Website A chatroom.<sup>8</sup> In the video, she first displays her breasts and then her genitals to the webcam. Later in the video, she inserts her fingers into her vagina before eventually inserting a hairbrush. The person recording this video recorded both the minor on webcam and the chat conversation and list of users in the chatroom when the victim engaged in sexually explicit conduct. **LAK** and **MATT** were both on the user list. Although the video that was recorded does not show any comments **LAK** might have made, it shows **MATT** giving the minor female directions, by telling her, "dinger that tight pussy," "finger\*," "2 fingers," and "go get your hairbrush; it will feel better than fingers." The minor female followed these directions. A screenshot from this video is shown below. The depiction of the minor female is redacted:

---

<sup>8</sup> The minor females in these videos have not been identified. The estimated ages provided are based on the training and experience of your affiant with these types of investigations looking at the primary sexual characteristics and facial features of the female depicted.



29. Second, a video entitled Untitled137.avi depicts a female believed to be between 14 and 17 years old on webcam in a Website A chatroom. In the video, she undresses and then displays her genitals to the webcam. Like the [MV].avi video above, the person recording this video recorded both the minor on webcam and the user list and chat below the webcam in the chatroom.

Among the users in that chat room were **LAK**, **MATT**, and **ZHIT**. All three users directed the minor female. At one point, **MATT** stated, “now get in all four,” **ZHIT** added, “doggy style [heart emoji],” and **MATT** said, “with your face down on the bed.” Later on, **ZHIT** told her, “peel that panties on the side with your thumb,” and **LAK** added, “slide the panties down hehe.” The username utilized by the minor female, Rawrrr, was only used on Website A on camera on October 31,

2015, through November 1, 2015, in the chatroom /funzchat. The same IP address identified below as being used by **LAK**, 172.12.52.227, was also observed to log into this room on those two days. A screenshot from this video is shown below.

The image of the minor female has been redacted:



30. Third, a video entitled [MV].avi depicts a female believed to be between 14 and 17 years old on webcam in a Website A chatroom. She showers and then, after drying herself with a towel, inserts her fingers into her vagina and masturbates. The recording included the minor on webcam and the chat conversation, but did not include the user list. From the chat conversations, it is evident that, at a minimum, Zhit group members **WHISPER20** and **ROB** were both in the room when this video

was made. At one point, a user with the generic username Dog\_248 states, “shes only 15... this is considered child porn; hahahahahahahhahhahaa.” Later, **WHISPER20** states, “nice body; mmmm” and, after she is done masturbating, both **WHISPER20** and **ROB** say thank you to her. A screenshot from this video is shown below. The image of the minor female has been redacted:



31. The FBI searched the logs from Website A for the usernames listed above that are associated with Zhit’s group. Through that search, the FBI discovered that several of those users consistently used the same IP address or a set of IP addresses associated with a specific geographical location to frequent Website A. For example, the

username **LAK** consistently used the IP address 172.12.52.227 from June 11, 2015, to near the end of the logs, September 3, 2017. Username **WHISPER20** consistently used the IP address 98.122.107.2 from August 25, 2015, to May 28, 2017. Username **TURTLE** used the IP address 99.90.82.117 from October 12, 2015, to near the end of the logs, September 17, 2017. Username **ZHIT** used a few different IP addresses, all of which geolocated to the Philippines. Username **PERP6969** also used a set of IP addresses, all of which geolocated to Portland, Oregon.

32. Moreover, consistent with their membership in the group, the logs showed that the IP addresses associated with these usernames, **PERP6969**, **ZHIT**, **WHISPER20**, **LAK**, and **TURTLE**, were frequently in the same chatrooms on the same days.

33. The FBI next analyzed what chatrooms on Website A these IP addresses consistently visited and were in at the same time as usernames associated with other group members. This analysis showed that much like how the Fans group used the word “fans” in the title of its chatrooms, Zhit’s group consistently used the word “chats” in naming its chatrooms on Website A. For example, an analysis of the logs, showed that this group used the following chatrooms, among others: justchat, wydchat, funnzchatz, supchat, mustchatxx, lovechatx, iwantchatxx, luvtochat, enjoychat, etc. Therefore, Zhit’s group will hereinafter be referred to as the “Chats group” and their chatrooms hereinafter will be referred to as the “Chats chatrooms.”



The FBI also discovered from the logs that other usernames associated with Zhit's group, including **MATT** or **MATTDUDE**, **CONNOR**, and **TBSTBS**, frequented Chats chatrooms.

***Minor victims' interactions with the Chats Group***

34. Beyond identifying Chats group members, the FBI's review of frequent IP addresses visiting Chats chatrooms also provided information about potential victims of the group. Several such victims have been identified. For example, Minor victim 1 (hereafter MV-1), a minor female born in the year 2000, resides in Ann Arbor, Michigan. MV-1 was on Website A from October 22, 2015, to January 30, 2016, in chatrooms named "hotchat4", "funzzchatz2", "chillme", "havingfun", and "wydchatxx." MV-1 was interviewed on February 10, 2017, and stated that she had visited Website A after being invited by an individual she met on a social media site called YouNow. Once she logged onto Website A, the conversation became sexual and the users in the chatrooms asked her to engage in sexual activity.

35. On August 24, 2017, MV-1 was interviewed again. MV-1 stated she created and shared explicit images over Skype with individuals she knew as Alexis, Theodore, and Ethan. MV-1 was not sure if she had exposed herself on webcam to a group on Website A but knew she had engaged in sexual activity on another similar

website and remembered having also done so on webcam in a chatroom on Website A with at least one of the individuals listed above who she knew from Skype. A review of the Skype conversations from MV-1's computer showed the Skype accounts of Alexis, Theodore, and Ethan to be lickingoreosx, imyourmom9, and nevereverblink, respectively. The FBI subpoenaed Skype for subscriber information related to these three usernames. Those results showed that the IP addresses used to login all matched IP addresses previously identified as belonging to Chats group member **ZHIT**.

***Identifying PERP6969 through Website A logs***

36. As stated above, one of the users identified by the Skype group as being a member of the Chats Group was **PERP6969**. In addition to the above conversation which references **PERP6969** by the Skype group, another comment which was dated as occurring on September 25, 2016 made reference to **PERP6969** by Skype username camilosucksdick, "[Minor victim's name] was linked long ago by her friend, and they were in our room and **PERP6969** group too, they said they liked the other guys more. [Username of potential minor victim] never do anything with us but she said she flashed and bated for the other group."

37. One of the individuals that has been identified as a member of this group, username **WHISPER20**, whose true name is Myron Brown was interviewed during

the execution of a search warrant at his residence on August 2, 2018. During the interview, Brown confirmed that he used the username **WHISPER20** on Website A. He identified a group that he had previously worked with on Website A to view child pornography which included **ZHIT** and **PERP6969**. Brown further stated that the user he knew as **PERP6969** was currently in his group on Website A working to obtain child pornography and that he believed that he resided in Washington state.

38. The analysis of the Website A logs showed that a user with username **PERP6969** consistently utilized IP addresses that geolocated in the vicinity of Portland, Oregon and were owned by CenturyLink. In fact a search of the IP addresses utilized on Website A to stream video on the site utilizing the username **PERP6969** showed that there were 32 separate IP addresses used to do so all of which are owned by CenturyLink and all of which geolocated to the vicinity of Portland, Oregon. These IP addresses were used to login to chatrooms on Website A from April 3, 2015 to September 30, 2017, extending for the entire period that logs from Website A are currently available. These IP addresses were utilized to login to approximately 1,075 different chatrooms on Website A a total of 9,113 times, including the Chats group chatrooms: /enjoychat, /enjoychatxx, /funchat, /heychat, /ilovechatx, /itsfunchat, /itsfunnchat, /iwantchat, /iwantchatx, /ixfunchatx /justchat, /letschat, /mustchatx, /mustchatxx, /nicechatx, /supchat, /wydchat, /wydchatx, /wydchatxx, /xfunchatx, and

/yeschat. The IP address was also used to stream on Website A, primarily with a SplitCam Video Driver or ManyCam Video Source in chatrooms named after Chats group members such as **PERP6969**, **ROB**, and **WHISPER20**, primarily with the username **PERP6969**, but also with the usernames numba1dad and trapper. These IP addresses were also used to login to the same rooms as MV-1 on several days when she logged into those rooms. Specifically the IP address 75.175.15.149 was used to log in to the Website A room /wydchatxx on January 27, 2016, and January 30, 2016, the same days that MV-1 was on camera in those rooms.

39. Further, these IP addresses, were used to login to chatrooms in which child pornography was produced during the undercover operation from December 3, 2015 to December 21, 2015. Particularly, a user with username **PERP6969** was observed to be in the chatroom /lexibluu on Website A on December 5, 2015 when an identified minor female, MV-12 with date of birth of April XX, 1999 was observed to masturbate while on webcam. The IP address 97.120.73.129, which is owned by CenturyLink and geolocates in the vicinity of Portland, Oregon, was found to have logged into this chatroom on December 5, 2015. Also, a user with username **PERP6969** was observed to be in the chatroom /sarina on Website A on December 16, 2015 when an unidentified minor female, who appears to be 13-15 years old was observed to have masturbated on webcam. The IP address 174.25.122.253 which

is owned by CenturyLink and geolocates in the vicinity of Portland, Oregon was found to have logged into this chatroom on December 16, 2015.

40. The FBI subpoenaed CenturyLink for subscriber information for three of the IP addresses that were logging into Website A Chats Group rooms with potential minor victims in September of 2016. The IP addresses requested were 184.100.236.191 on April 7, 2016, 184.100.218.73 on April 13, 2016, and 174.25.96.63 on April 15, 2016. CenturyLink provided responsive material which showed that the subscriber for all three IP addresses was **Richard Eby**, 532 NW Everett Street, Apartment 418, Portland, Oregon 97209.

41. A check of open source information showed that the only resident at 532 NW Everett Street, Apartment 418, Portland, Oregon 97209 was **Richard J Eby**, date of birth XX/XX/1962. A check of criminal history was negative for **Eby**. A check of the Oregon sex offender registry was negative for both **Eby** and the address.

42. The FBI requested a pen register/trap and trace device (PR/TT) for the internet service at 532 NW Everett Street, Apartment 418, Portland, Oregon 97209 pursuant to a 2703(d) Court Order. This PR/TT went active on or about March 10, 2017. A review of the data obtained shows a user of the internet at the residence utilizing the IP address 70.57.124.1 to access Website A. This IP address was used by an Internet user at the residence until January 16, 2018. This same IP address, 70.57.124.1, was

found to be utilized by an individual utilizing the username **PERP6969** on Website A from at least March 2, 2017 to September 30, 2017, based on the logs from Website A. Communication with Centurylink regarding the PR/TT determined that on January 18, 2018, the service was terminated at this address.

43. Open source searches found a Twitter account with the username **PERP6969** which had the display name set as **Richard Eby**. An administrative subpoena was served on Twitter for subscriber data of this account. Twitter responded on July 26, 2018 with information that showed that the associated email address with the account was [perpwontdie@gmail.com](mailto:perpwontdie@gmail.com). The recent IP logins to this account were found to geolocate to Medellin, Colombia. Google was subpoenaed for subscriber information for the email address [perpwontdie@gmail.com](mailto:perpwontdie@gmail.com) and they responded with subscriber information on August 9, 2018 which showed the subscriber was **Richard Eby** and recent IP logins had come from IP addresses geolocated to Bogata, Colombia. There was also a cellular telephone associated with the account with telephone number 971-322-8360. Verizon Wireless was found to own the telephone number and an administrative subpoena requesting subscriber information was served on August 13, 2018. On August 14, 2018, Verizon Wireless provided subscriber information for the telephone number as **Richard J Eby** at residence address 532 NW Everett Street,

Apartment 418, Portland, OR 97209. It further showed that service for **Eby** to this telephone number had been disconnected on June 25, 2018.


44. Your affiant concluded based on the forgoing that **Eby** had departed the country and was currently residing in Colombia. Your affiant requested that he be notified when **Eby** returned to the United States. On June 25, 2019, U.S. Customs and Border Patrol (CBP) notified your affiant that **Eby** was scheduled to arrive at the Fort Lauderdale-Hollywood International Airport from Colombia. When **Eby** arrived in the United States, CBP determined that there was potential child pornography material on **Eby's** electronic devices, and Homeland Security Investigations (HSI) seized them.

45. On September 20, 2019, the devices seized from **Eby** were transferred to the custody of the FBI in Detroit, Michigan. These included the three SUBJECT DEVICES: a Samsung SM-J320V cellular telephone bearing IMEI 359260072747840, an Acer Aspire ZRQ laptop bearing serial number NXMEFAA004409008007600, and an Ativa SD 60x 2GB SD card. These devices remain in the custody of FBI in Detroit, at the location specified in Attachment A.

**CONCLUSION**

46. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the location specified in Attachment A in the Eastern District of Michigan. I respectfully request that this Court issue a search warrant for the items in Attachment A, authorizing the seizure and search of the items described in Attachment B.

Respectfully submitted,

  
\_\_\_\_\_  
Special Agent Adam Christensen  
Federal Bureau of Investigation

Sworn to via telephone after submission by reliable electronic means. Fed R. Crim. P. 4.1 and 41(d)(3).

  
\_\_\_\_\_  
Hon. R. Stephen Whalen  
United States Magistrate Judge

Date:     October 3, 2019



**ATTACHMENT A**  
**DESCRIPTION OF EVIDENCE TO BE SEARCHED**

The following items, which were seized by the Homeland Security Investigations from Richard Eby on June 26, 2019 at Fort Lauderdale-Hollywood International Airport when he arrived in the United States from Colombia, which are now in the custody of the Federal Bureau of Investigation in Detroit, Michigan which is in the Eastern District of Michigan:

- Samsung SM-J320V cellular telephone bearing IMEI 359260072747840;
- Acer Aspire ZRQ laptop bearing serial number NXMEFAA004409008007600;
- Ativa SD 60x 2GB SD card.

**ATTACHMENT B**  
**Information to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A, Title 18 United States Code, Section 2251(a) and (e), and Title 18 United States Code Section 2422:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereafter, “COMPUTER”):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;

- d.** evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e.** evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f.** evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g.** evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h.** evidence of the times the COMPUTER was used;
- i.** passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j.** documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k.** records of or information about Internet Protocol addresses used by the COMPUTER;
- l.** records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m.** contextual information necessary to understand the evidence described in this attachment.

3. Child pornography and child erotica.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

for the  
Eastern District of Michigan

one Samsung SM-J320V cellular phone, one Acer Aspire ZRQ laptop, and one Ativa SD card (more fully described in Attachment A)

Case: 2:19-mc-51458 - 1

Case No. Assigned To : Edmunds, Nancy G.

Assign. Date : 10/3/2019

IN RE: SEALED MATTER (CMC)

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ Michigan \_\_\_\_\_.  
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

**YOU ARE COMMANDED** to execute this warrant on or before October 16, 2019 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for            days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of           

Date and time issued: October 3, 2019 4:50 pm

City and state: Detroit, Michigan

*Judge's signature*

Hon. R. Steven Whalen, U. S. Magistrate Judge  
*Printed name and title*

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*